

CLAIMS

1. A method for data type preserving encryption of a data element in a relational database, wherein said  
5 database comprises a plurality of data elements of at least one type, and each data element comprises a string of at least one character, comprising the steps of:

reading the type of a data element which is to be encrypted;

10 interpreting said data type in order to form a restricting character set for each character of said data element;

encrypting each character of said data element into an encrypted character using said restricted character  
15 set to control the encryption process to only create encrypted characters included said restricted character set.

2. A method according to claim 1, comprising the  
20 further step of:  
arranging one or more character sets in a pattern for a data type.

3. A method according to claim 1 or 2, where the  
25 encryption results in a data element having the same number of characters as the unencrypted data element.

4. A method according to claim 1, comprising the further steps of:  
30 converting each character to an index value; and  
adding a varying value to each index value before encryption.

5. A method according to claim 4, wherein the  
35 varying integer value is obtained by the steps of:  
creating an initial value by hashing the encryption key;

adding adjacent index values pairwise from the left to the right using said initial value when adding the leftmost character.

- 5           6. A method according to claim 1, wherein the encryption is performed using the DES algorithm in stream cipher mode.

- 10           7. A system for data type preserving encryption of a data element in a relational database, which database comprises a plurality of data elements of at least one type, and each data element comprises a string of at least one character, comprising:

- 15           reading means for reading the type of a data element which is to be encrypted;

            interpretation means for interpreting said data type in order to form a restricting character set for each character of said data element;

- 20           encryption means for encrypting each character of said data element into an encrypted character using said restricted character set to control said encryption means to only create encrypted characters included said restricting character set.